PCT/EP00/04141

BUNDESREPUBLIK DEUTSCHLAND

EP00/04141

09/926460

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

4

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	199 21 524.3
Anmeldetag:	10. Mai 1999
Anmelder/Inhaber:	Giesecke & Devrient GmbH, München/DE
Bezeichnung:	Einrichtung zum Schutz des Ersteinsatzes einer Prozessor-Chipkarte
IPC:	H 04 Q, H 04 L, G 06 K

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 27. Juni 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hoiß

A 9161
03/00
EDV-L

Einrichtung zum Schutz des Ersteinsatzes einer Prozessor-Chipkarte

Die Erfindung betrifft ein Verfahren zum Schutz vor Angriffen auf eine Prozessor-Chipkarte beziehungsweise deren nicht autorisierten Einsatz in einem Netzwerk zur Nachrichtenübertragung, vorzugsweise einem GSM-Netzwerk nach dem Oberbegriff des Anspruchs 1 sowie eine entsprechende Chipkarte nach dem Oberbegriff des Anspruchs 9.

Bei GSM-Systemen ist es bekannt, daß sich zum Einsatz der Chipkarte (Subscriber Identity Module SIM) zunächst der Kartenbenutzer mittels einer persönlichen Identifikationsnummer (PIN) als zur Benutzung berechtigt ausweisen muß. Um an dieser Stelle Mißbrauch zu vermeiden, ist es für die PIN-Übermittlung an den Kartenbenutzer bekannt, PIN/PUK-Briefe durch den Kartenhersteller oder den Kartenpersonalisierer herstellen zu lassen und diese PIN/PUK-Briefe an den Kartenbenutzer auszuhändigen.

Eine weitere, systemrelevante Sicherheitsmaßnahme besteht in der Versiegelung des PIN/PUK-Briefs durch den Kartenhersteller oder Kartenpersonalisierer. Die Unversehrtheit des Siegels auf dem PIN/PUK-Brief zeigt dem Kartenbenutzer an, daß keinem anderen Kartenbenutzer die beim Kartenhersteller auf den PIN/PUK-Brief aufgebrachten Geheimnummern bekannt sein können. Da die Geheimnummern auf dem PIN/PUK-Brief durch den Kartenhersteller oder Kartenpersonalisierer zufällig gewählt wurden und nur noch im geheimen Speicher der SIM-Karte abgelegt sind, kann der Kartenbenutzer davon ausgehen, daß durch Öffnung des PIN/PUK-Briefs nur er selbst in Kenntnis der Geheimnummern gelangt.

Um bei der PIN-Eingabe Mißbrauch zu vermeiden, ist es für die PIN-Eingabe bekannt, einen Fehlerzähler vorzusehen, der nach Überschreitung einer zulässigen Anzahl von Fehlversuchen den weiteren Gebrauch der Karte vorläufig unterbindet. Zum Schutz des unnötigen Sperrens einer Karte durch versehentliche Falscheingabe der PIN ist es bekannt, auf der Karte einen

Personal Unblocking Key (PUK) vorzusehen, mit dessen Hilfe die Festlegung einer neuen PIN möglich ist und der die Karte für den Einsatz im Netzwerk wieder freischaltet. Um bei der PUK-Eingabe Mißbrauch zu vermeiden, ist es bekannt, einen Fehlerzähler vorzusehen, der nach Überschreitung einer zulässigen Anzahl von Fehlversuchen den weiteren Gebrauch der Karte endgültig unterbindet.

Bei dem bekannten Stand der Technik wird dem Kartenbenutzer die Möglichkeit eingeräumt, die einmal durch den Kartenhersteller oder Kartenpersonalisierer festgelegte PIN durch einen selbstgewählten Wert zu ersetzen. Der Wert des PUK kann vom Kartenbenutzer nicht verändert werden. Um dem Kartenbenutzer bei Verlust oder nicht greifbarem PIN/PUK-Brief, aber versehentlich gesperrter PIN, den PUK dennoch mitteilen zu können, ist es bekannt, als besondere Dienstleistung in manchen GSM-Netzen den PUK zusätzlich in einer Datenbank zentral beim Netzbetreiber für alle herausgegebenen Karten zu speichern. Auf Anfrage durch den Kartenbenutzer und nach Überprüfung der Identität des Kartenbenutzers wird der PUK zur Freischaltung der PIN dem Kartenbenutzer mitgeteilt.

Auch in einem derartigen System besteht die Gefahr, daß durch unerlaubte Öffnung des PIN/PUK-Briefs und beispielsweise durch Neudruck des PIN/PUK-Briefs oder durch Manipulation des PIN/PUK-Brief-Siegels der rechtmäßige Kartenbenutzer im Glauben ist, Erstbenutzer der Karte zu sein, obwohl bereits vorher ein unrechtmäßiger Kartenbenutzer die Karte auf Kosten des rechtmäßigen Kartenbenutzers vorübergehend in Betrieb genommen hat.

Es ist deshalb Aufgabe der Erfindung, ein sicheres Verfahren zum Schutz vor unbemerkter Öffnung von PIN/PUK-Briefen, bei dem der Erstbenutzer der

Karte über die Erstbenutzung der Karte in Kenntnis gesetzt wird sowie eine entsprechende Chipkarte anzugeben.

Diese Aufgabe wird ausgehend von den Merkmalen des Oberbegriffs des Anspruchs 1 bzw. 9 durch die jeweiligen kennzeichnenden Merkmale gelöst. Vorteilhafte Ausgestaltungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

Die Erfindung betrifft ein Verfahren zur Überprüfung und Anzeige des Ersteinsatzes einer Prozessor-Chipkarte mittels einer Zusatzanwendung auf der Prozessor-Chipkarte selbst, die alle zur sicheren Prüfung notwendigen Schritte steuert oder zumindest wesentlich beeinflußt.

Eine vorteilhafte Ausgestaltung der Erfindung zeigt den Einsatz der Applikation, um geheime Schlüssel, die zur Authentifikation des Kartenbenutzers gegenüber der Karte benötigt werden, durch den Kartenbenutzer festlegen zu lassen oder dem Kartenbenutzer diese Schlüssel mitzuteilen, wobei die Karte auf dem Weg zwischen Kartenhersteller, Kartenherausgeber und Kartenbenutzer transportgesichert bleibt.

Ein weiterer vorteilhafter Einsatz der Erfindung ist die Ergänzung oder der Ersatz von aufwendigen und teils kostenintensiven Verfahren zur Transportsicherung von Prozessor-Chipkarten zwischen Kartenhersteller und Kartenbenutzer, wie zum Beispiel PIN/PUK-Briefen, durch die Zusatzanwendung in der Prozessor-Chipkarte, welche die Aufgabe eines PIN/PUK-Briefs ergänzt oder im wesentlichen übernimmt.

Gemäß einer weiteren vorteilhaften Ausführungsform kann die Erfindung auch als Bestandteil eines in wesentlichen Teilen in der Prozessor-Chipkarte selbst ablaufenden Systems zur individuellen Vergabe und Personalisierung

von geheimen Schlüsseln eingesetzt werden, die nicht nur dem Kartenbenutzer, sondern auch dem Kartenherausgeber, etwa einem Mobilfunknetz-Betreiber oder Netzdienste-Anbieter, zugänglich gemacht werden sollen.

Eine weitere vorteilhafte Ausgestaltung der Erfindung sieht vor, daß bei Festlegung der Geheimschlüssel durch den Kartenbenutzer selbst, diese geheimen Schlüssel mehrmals vom Kartenbenutzer abgefragt werden, um eine versehentliche Falscheingabe zu vermeiden.

Alternativ oder zusätzlich kann nach Festlegung der Geheimzahlen durch den Kartenbenutzer oder durch die Karte selbst, einer entsprechende Netzwerkkomponente eine Information übermittelt werden, wonach im Netzwerk der Ersteinsatz der Karte mitgeteilt oder der Wert der Geheimnummer übermittelt wird.

Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung werden bei Erstinbetriebnahme der Karte die Geheimzahlen zusätzlich oder alternativ über die Sprach- oder Hörvorrichtung des Mobilfunkgeräts ein- oder ausgegeben, wodurch insbesondere die Übermittlung oder Festlegung der geheimen Schlüssel an oder durch sehbehinderte Kartenbenutzer erleichtert und besser gesichert werden kann.

Die Fig. 1 zeigt ein Ausführungsbeispiel einer Chipkarte SIM, die eine Schnittstelle S zum Datenaustausch mit einem Mobilfunktelefon aufweist sowie einen Mikroprozessor µP, der mit einer Applikation A und einem Speicher M, Mg verbunden ist. Die Applikation A kann im wesentlichen als SIM Application Toolkit Applikation ausgebildet sein und ist durch den Kartenhersteller oder Kartenpersonalisierer in die Karte eingebracht worden. Der Speicher ist unterteilt in den üblichen Speicherbereich M, in dem Daten

ausgelesen und eingeschrieben werden können und in den geheimen Speicherbereich Mg, in dem zumindest die Information über den Ersteinsatz der Chipkarte abgelegt ist. Wenn über die Schnittstelle S die Karte durch einen Kartenbenutzer in Betrieb genommen wird, so prüft die Applikation mittels Zugriff auf den geheimen Speicher Mg, ob es sich um den Ersteinsatz der Karte handelt.

Bei Ersteinsatz der Karte wird der Kartenbenutzer durch die Applikation A informiert und zur Bestätigung der Inbetriebnahme der Karte aufgefordert. Bei positiver Bestätigung durch den Kartenbenutzer ändert die Applikation die Information über den Ersteinsatz im geheimen Speicher Mg und verändert dadurch ihr Verhalten bei einer späteren Wieder-Inbetriebnahme der Karte.

Patentansprüche

1. Verfahren zur Inbetriebnahme einer Prozessor-Chipkarte für ein Netzwerk zur Nachrichtenübermittlung, vorzugsweise einem GSM-Netzwerk, bei dem sich der Kartenbenutzer gegenüber der Prozessor-Chipkarte (SIM) durch eine persönliche Geheimnummer ausweisen muß **dadurch gekennzeichnet, daß**

- zur Ablaufsteuerung des Ersteinsatzes zunächst die Prozessor-Chipkarte beim Kartenhersteller oder Karten-Personalisierer mit einer Zusatzapplikation, vorzugsweise unter Verwendung des SIM Application Toolkit, versehen wird, die den Einsatz zur Benutzung im Netzwerk verhindert und statt dessen nur einen lokalen Einsatz mittels Kartenleser oder Kartenterminal, vorzugsweise einem Mobilfunkgerät erlaubt, und
- bei Ersteinsatz der Prozessor-Chipkarte die Applikation ohne weitere Prüfung einer Geheimzahl ein Anzeigesignal für die Erstbenutzung und eine Bestätigungsanforderung ausgibt, und
- nach Erhalt eines Bestätigungssignales die Zusatzapplikation deaktiviert oder deren Ablauf so verändert wird, daß beim nächsten Einsatz der Karte ein Anzeigesignal ausgegeben wird, welches angibt, daß die Erstinbetriebnahme bereits erfolgt ist, und der Einsatz der Prozessor-Chipkarte im Netzwerk freigegeben wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, daß** zur Aktivierung der Zusatzapplikation eine vorher, bevorzugt durch den Kartenhersteller oder Karten-Personalisierer, festgelegte persönliche Geheimzahl eingegeben werden muß.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, daß** nach Ersteinsatz der Karte und vor Deaktivierung oder Zustandsänderung der Zusatzapplikation die Eingabe einer persönlichen Geheimzahl (PIN) und /oder einer Geheimzahl (PUK) für die Änderung oder Entsperrung der persönlichen Geheimzahl (PIN) angefordert wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, daß** einzelne oder alle persönlichen Geheimzahlen auf der Karte bereits durch den Kartenhersteller auf der Prozessor-Chipkarte personalisiert wurden und diese Geheimzahlen beim Ersteinsatz zum späteren Gebrauch am Kartenleser oder Kartenterminal, vorzugsweise einem Mobilfunkgerät, angezeigt werden.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, daß** einzelne oder alle persönlichen Geheimzahlen auf der Karte durch einen in der Karte eingebauten Zufallszahlengenerator vorgegeben werden und diese Geheimzahlen während des Ersteinsatzes am Kartenleser oder Kartenterminal, vorzugsweise einem Mobilfunkgerät, angezeigt werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, daß** einzelne oder alle persönlichen Geheimzahlen zur Übermittlung an das Netzwerk, vorzugsweise in verschlüsselter Form über einen Datenkanal, zusammengefaßt und unmittelbar oder zu einem späteren Zeitpunkt an eine zentrale Stelle beim Netzbetreiber oder Netzdienste-Anbieter gesendet werden.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, daß** die bei der Erstinbetriebnahme festzulegenden Geheimzahlen nicht zum Zweck des Schutzes der Netzwerk-Applikation sondern zum Schutz einer

Zusatzapplikation, bevorzugt einer SIM Application Toolkit Applikation, auf der SIM Karte verwendet werden.

8. Verfahren nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet,** daß Informationen über den Ersteinsatz der Prozessor-Chipkarte und über die persönlichen Geheimzahlen über die Hör- oder Spracheinrichtungen des Kartenlesers, des Kartenterminals oder vorzugsweise des Mobilfunkgeräts aus- oder eingegeben werden.

9. Chipkarte mit einem Mikroprozessor (µP), einem Speicherbereich (M) und einer Schnittstelle (S), welche jeweils mit dem Mikroprozessor (µP) verbunden sind, **gekennzeichnet durch** einen Speicherbereich (A), in dem eine Anwendung zur Ablaufsteuerung des Ersteinsatzes der Chipkarte abgelegt ist und einem geheimen Speicherbereich (Mg), in dem Daten zu dieser Anwendung gesichert abgelegt sind.

Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Inbetriebnahme einer Prozessor-Chipkarte in einem Netzwerk zur Nachrichtenübermittlung, vorzugsweise in einem GSM-Netzwerk, bei dem sich der Kartenbenutzer gegenüber der Prozessor-Chipkarte (SIM) durch eine persönliche Geheimzahl ausweisen muß.

Gemäß der Erfindung ist auf der Chipkarte eine Applikation gespeichert, welche den Ablauf beim Ersteinsatz der Prozessor-Chipkarte durch den Kartenbenutzer steuert. Die Applikation wird zur Übermittlung eines Hinweises über die Erstbenutzung an den Kartenbenutzer eingesetzt. In einem weiteren Ausführungsbeispiel der Applikation, wird diese Applikation dazu eingesetzt, persönliche Geheimzahlen zum nachfolgenden Einsatz der Prozessor-Chipkarte im Netzwerk an den Karten-Erstbenutzer zu übermitteln oder durch den Karten-Erstbenutzer festlegen zu lassen.

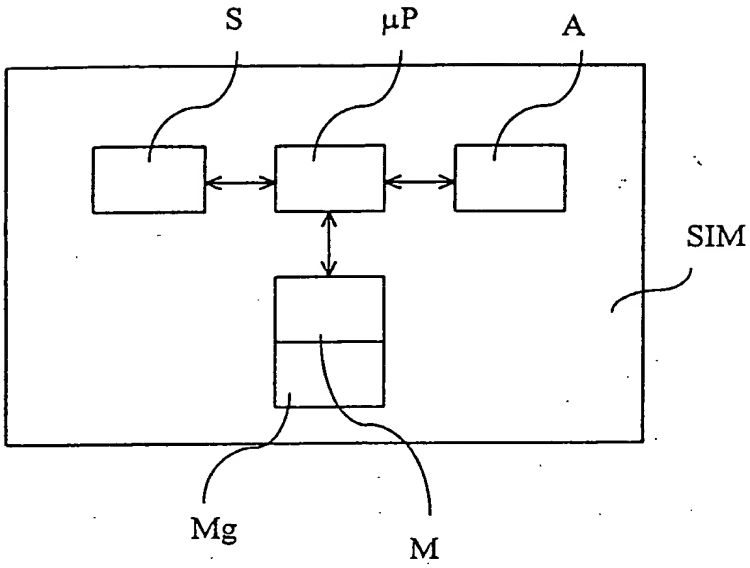

Fig. 1